Général : **(7 pts)**

Q1 : Expliquez ce qu'est la technologie RAID et quels sont les critères de performance sur lesquels les différents niveaux de RAID se démarquent.

0,5 *La technologie RAID consiste à agréger plusieurs disques durs de façon à améliorer les performances ou la tolérance aux pannes. Il existe différents niveaux de RAID correspondant à différents agencements des disques durs.*

0,5
- *Rapport entre la capacité logique utilisable et la capacité physique des disques.*

0,5
- *Le nombre de disque pouvant tomber en panne sans perdre l'accès aux informations.*

0,5
- *Le facteur d'accélération sur les opérations de lecture.*

Q2 : Quels sont les solutions technologiques utilisables pour faciliter l'administration d'un parc de machine ?

3,0 *On trouve des solutions :*

- *De prise de contrôle à distance permettant d'accéder à distance aux ressources de la machines (clavier, écran, …) pour pouvoir l'administrer sans se déplacer physiquement.*
- *De télédistribution de logiciels permettant d'installer, de mettre à jour ou de supprimer à distance un programme d'un ensemble de machines du parc.*
- *De supervision globale de l'état du Réseau (tel que HP OpenView), permettant de récolter des informations via le protocole SNMP (nombre de collisions, table de routage, consommation CPU, …).*
- *De définition centralisée de la politique d'administration d'un logiciel tel qu'un antivirus (F-secure par exemple).*
- *De fabrication d'images disques. Un serveur pourra contenir plusieurs versions d'images des disques durs d'un parc et pourra les transférer sur un ensemble défini de machines, via le multicast (Les CD ou DVD peuvent également être une solution pour la réinstallation d'une machine depuis le master).*
- *De client léger et de serveur d'application pour centraliser l'administration et banaliser la gestion du parc.*
- *De SAN de NAS avec robot de sauvegarde pour centraliser les données (s'appuyant sur l'accès disque à distance en utilisant CIFS (ex SMB) ou NFS, …) et les sauvegarder*
- *De sauvegarde à distance (solution client/serveur pour la sauvegarde de données distribuées vers un serveur disposant du robot de sauvegarde.*
- *D'annuaires pour la centralisation des comptes utilisateurs (Contrôleurs de domaines, LDAP, NIS, DNS, …).*

Notation : 0,5 point par réponse valide ; bornée à un total de 3 points.

Q3 : Quels sont les intérêts des technologies de virtualisation ?

2,0

- *Cela permet de tester plusieurs configurations systèmes sans perturber la configuration de la machine réelle qui sera utilisée.*
- *Cela permet d'héberger sur une même machine réelle plusieurs machines virtuelles (cas d'un provider offrant des serveurs à ces clients) dès lors que chacune des machines virtuelles n'a pas besoin d'utiliser une part importante de la puissance d'une machine physique. → diminution du coût matériel, du coût électrique.*
- *Maquettage de plusieurs machines sur un même ordinateur pour faire des présentations ou des formations sur des environnements nécessitant normalement plusieurs machines.*
- *Snap-shot de l'état des disques offert par la virtualisation sans que le système d'exploitation, des machines virtuelles, n'ait à le gérer (Disques de différentiation ou disques d'annulation de virtualPC par exemple).*
- *Snap-shot de l'état des machines virtuelles*

Notation : 1 point pour chaque réponse, borné à un total de 2 points.

<u>Apache :</u> (4 pts)

Dans le fichier « `httpd.conf` », on trouve la section suivante :

```
  <Directory "/www ">
    Options FollowSymLinks Indexes
    AllowOverride None
  </Directory>
```

Q4 : Que doit-on ajouter dans la section présentée ci-avant pour que l'accès au répertoire /www ne soit autorisé que pour :

- la machine localhost (`127.0.0.1`),
- les machines du sous réseau `10.27.12.0/24`,
- les machines d'adresse ip comprises entre `192.168.1.33` et `192.168.1.35`,
- les machines de la classe C `195.220.73.0` à l'exception de la machine d'adresse `195.220.73.23`.

Rappel : Il faut spécifier des règles d'autorisation et d'interdiction (access-list) via les directives « Allow » et « Deny ». Il faut également utiliser la directive « Order » pour spécifier l'ordre d'examen des directives « allow » et « deny »

0,5

Le cahier des charges spécifie une restriction par défaut pour les machines qui ne sont pas autorisées via les autres règles. La directive « order » doit donc être utilisée de la façon suivante :

```
Order allow, deny
```

0,5

« Autorisé pour la machine localhost (127.0.0.1) » se traduit par :

```
Allow from 127.0.0.1
```

« Autorisé pour les machines du sous réseau 10.27.12.0/24 » se traduit au choix par :

```
Allow from 10.27.12
```

ou

```
Allow from 10.27.12.0/24
```

ou

```
Allow from 10.27.12.0/255.255.255.0
```

0,5 *La plage 192.168.1.33 à 192.168.1.35 ne peut être décrite directement. Cela ne correspond pas à un subnet. Il faudra donc le décrire comme une liste de machines ou une liste de subnets. Les adresses 192.168.1.34 et 192.168.1.35 peuvent être regroupées en spécifiant 192.168.1.34/31 mais 192.168.1.33 restera seul. « Autorisé cette plage » se traduit donc par :*

```
Allow from 192.168.1.33/32
Allow from 192.168.1.34/32
Allow from 192.168.1.35/32
```

ou

```
Allow from 192.168.1.33/32
Allow from 192.168.1.34/33
```

0,5 *« Autoriser la classe C 195.220.73.0 à l'exception de 195.220.73.23 » nécessite d'écrire une règle d'autorisation de la classe C et une règle d'interdiction (conformément à la directive « Order » spécifiée plus haut, les règles d'interdictions définissent des exceptions aux règles d'autorisations) :*

```
Allow from 195.220.73.0/24
Deny from 195.220.73.23/32
```

Soit l'ensemble des règles :

```
Order allow, deny
Allow from 127.0.0.1
Allow from 10.27.12.0/24
Allow from 192.168.1.33/32
Allow from 192.168.1.34/33
Allow from 195.220.73.0/24
Deny from 195.220.73.23/32
```

Remarque : L'ordre d'écriture des règles n'a pas d'importance.

Q5 : Comment fait-on si on veut définir des droits d'accès par utilisateur (login/mot de passe) ? (Est-ce possible ?)

1,0 *Oui il est possible de définir des droits d'accès par utilisateur. Le protocole http permet l'envoi dans chaque requête d'une authentification (login/mot de passe). Cette authentification peut être vérifiée par apache. Il suffit d'utiliser les directives « AuthType », « AuthName », « AuthUserFile » et « Require ».*

- *« AuthType » permet de spécifier le type d'authentification que devra utiliser le protocole http. Exemple :*
  ```
  AuthType Basic
  ```
- *« AuthName » permet de spécifier un nom de domaine d'authentification (Le navigateur peut ainsi mémoriser des authentifications différentes en fonction de ce nom). Exemple :*
  ```
  AuthName "Administration System Reseau"
  ```
- *« AuthUserFileName » permet de spécifier le fichier contenant la liste des utilisateurs et leurs mots de passe cryptés. Remarque : il est également possible de coupler l'authentification avec un annuaire LDAP (mais ce n'est pas l'objet de la question).*
- *« Require » permet de spécifier d'un utilisateur valide est nécessaire (ou que l'utilisateur fasse parti de la liste des utilisateurs ou des groupes spécifiés).*
  ```
  Require valid-user
  ```

Il est également possible de ne pas définir les droits d'accès dans « Apache » et de laisser à un script « php » le filtrage des requêtes puisque « Apache » transmet à l'interpréteur « php » les informations issus du protocole http (mais on sort du cadre de la question).

Q6 : Quelle est l'utilité des sections « VirtualHost » dans les fichiers de configuration d'apache ?

1,0

Les sections « VirtualHost » permettent la configuration d'un serveur apache de telle sorte qu'il puisse fonctionner de façon différent (différence de contenu, …) suivant le nom du serveur demandé, le port contacté ou l'adresse IP contacté. Un unique apache peut donc simuler une collection de serveurs web.

<u>Sendmail :</u> (4 pts)

Soit la section S27 d'un fichier de configuration sendmail.cf contenant le code suivant :
Dans le fichier « `httpd.conf` », on trouve la section suivante :

```
S27
 R$*.$-@$*.domain.fr    $@$1.$2@domain.fr
 R$*@$*.domain.fr       $@$1@$2.domain.fr
 R$*@$*                 $1@$2
```

Q7a :Comment la section S27 réécrit-elle « login@machine.domain.fr » ?

1,0

*« **login@machine.domain.fr** » ne vérifie pas la première règle. On passe donc à la règle suivante.*

*« **login@machine.domain.fr** » vérifie la seconde règle :*

*« **$*** »*	*correspond à « **login** »*	*1ère élément*
« @ »	*correspond à « @ »*	
*« **$*** »*	*correspond à « **machine** »*	*2ème élément*
*« **.** »*	*correspond à « **.** »*	
*« **domain** »*	*correspond à « **domain** »*	
*« **.** »*	*correspond à « **.** »*	
*« **fr** »*	*correspond à « **fr** »*	

*L'adresse email est donc réécrite en « **login@machine.domain.fr** » et on arrête S27 (à cause de « **$@** ».*

Q7b :Comment la section S27 réécrit-elle « prenom.nom@labo.domain.fr »

1.0

*« **prenom.nom@machine.domain.fr** » vérifie la première règle :*

*« **$*** »*	*correspond à « **prenom** »*	*1er élément*
*« **.** »*	*correspond à « **.** »*	
*« **$-** »*	*correspond à « **nom** »*	*2ème élément*
« @ »	*correspond à « @ »*	
*« **$*** »*	*correspond à « **labo** »*	*3ème élément*
*« **.** »*	*correspond à « **.** »*	
*« **domain** »*	*correspond à « **domain** »*	
*« **.** »*	*correspond à « **.** »*	
*« **fr** »*	*correspond à « **fr** »*	

*L'adresse email est donc réécrite en « **prenom.nom@domain.fr** » et on arrête S27 (à cause de « **$@** ».*

Q8 : Que faut-il modifier (ou ajouter) à la section S27 pour que « login@machine.domain.fr » soit réécrit en « login@domain.fr » quand la machine est une machine de la liste suivante : « titi », « bip-bip », « bugs-bunny », « jerry » défini dans la classe « M ».

1.0 *Comme on l'a vu à la question Q7a, « **login@machine.domain.fr** » ne vérifie pas la première règle mais vérifie la seconde règle. La seconde règle ne réécrit pas cet email de la façon demandée, il va donc falloir insérer la règle suivante entre la première et la seconde règle :*

```
R$*@$=M.domain.fr       $@$1@domain.fr
```

*« **login@machine.domain.fr** » ne vérifie pas la seconde règle (la nouvelle) car « **machine** » n'est pas défini dans la classe M.*
*Mais « **login@machine.domain.fr** » vérifie la troisième règle (ex seconde règle).*
*Par contre « **login@titi.domain.fr** » vérifie la seconde règle :*

*« **$*** »*	*correspond à « **login** »*	*1ère élément*
« @ »	*correspond à « @ »*	
*« **$=M** »*	*correspond à « **titi** »*	*2ème élément*
*« **.** »*	*correspond à « **.** »*	
*« **domain** »*	*correspond à « **domain** »*	
*« **.** »*	*correspond à « **.** »*	
*« **fr** »*	*correspond à « **fr** »*	

*L'adresse email est donc réécrite en « **login@domain.fr** » et on arrête S27 (à cause de « **$@** ».*

Q9 : Quel est le rôle du fichier « .forward » ? Que permet-il de faire ?

1.0 *Le fichier « .forward » à pour rôle de rediriger des mails. A chaque utilisateur est associé un fichier « .forward » qui définira (quand il existe) comment le mail est être redirigé.*
Il permet la redirection vers une ou plusieurs boîtes mail et vers des programmes (ou filtre) interprétant le mail.
Le filtre reçoit alors le mail depuis « stdin » et pourra agir en fonction du contenu reçu.

<u>LDAP :</u> (4,0 pts)

Q10 :Quelle est la différence entre une base de données et un annuaire ?

1,0 *Bien que tous deux soient conçus pour mémoriser des données et les donner aux clients qui en font la demande, leur utilisation est différente. En effet :*

- *le rapport lecture/écriture est beaucoup plus élevé pour un annuaire (On fait beaucoup plus d'écriture – de mise à jour- dans une base de données)*
- *la diffusion des données d'un annuaire est beaucoup plus large (plus de clients pouvant s'y connecter)*
- *une normalisation (standard LDAP) des protocoles de communication des annuaires*
- *une distribution des données entre serveurs plus facile (à cause du faible taux d'écriture), réplication, cache augmentant : la fiabilité, les performances, la proximité des clients*
- *Performance globales des annuaires plus élevées tant que l'on reste dans leur domaine d'utilisation : les opérations de lecture et non d'écriture.*

Q11 :Quelle est la différence entre « le modèle d'information » et « le modèle de nommage » ?

1,5

Le modèle d'information défini la nature (autrement dit le type) des objets, que l'on pourra stocker dans l'annuaire, en spécifiant la liste des attributs et leurs caractéristiques.

Le modèle de nommage définit comment sont organisées (ou référencées) les entrées de l'annuaire.

Le « schéma » définit la structure du modèle d'information en spécifiant les relations d'héritage entre les objets (notion de classe d'objet).
Le DIT « Directory Information Tree » respectant l'organisation hiérarchique des données fixée par le modèle de nommage contient l'ensemble des entrées de l'annuaire (chaque entrée pouvant être de l'un des types définis dans le modèle d'information).

Remarque : La nature de ces deux hiérarchies est différente et indépendante.

Q12 :Comment est assurée la sécurité dans LDAP ?

1,5

La sécurité dans LDAP se fait à trois niveaux :

- *par l'authentification pour se connecter au service (c'est-à-dire la reconnaissance du client par le serveur afin d'éviter la connexion d'agent extérieur indésirable) ;*
- *par le modèle d'accès aux données (sortes d'« access-list ») qui fixe, par utilisateur, des droits d'accès aux données en fonction des opérations de lecture, d'écriture, de recherche et de comparaison agissant sur les entrées ou sur certains de leurs attributs ;*
- *par le chiffrement des transactions entre clients et serveurs et entre serveurs (cela protège contre l'interception de communication, celle-ci étant cryptée).*

DNS : (5 pts)

Q13 :Comment peut-on obtenir via le DNS la liste des serveurs de messagerie d'un domaine ? Choisissez la commande « `dig` » ou « `host` » et donnez la syntaxe à utiliser pour obtenir cette réponse dans le cas du domain « `fupl.asso.fr` »

1,0

Pour obtenir la liste des serveurs de messagerie d'un domaine, il faut rechercher les RR de type MX concernant ce domaine.

Si on utilise la commande « dig », on exécutera :

```
dig -t MX fupl.asso.fr
```

Si on utilise la commande « host », on exécutera :

```
host -t MX fupl.asso.fr
```

Une entreprise utilise les 2 SUBNET « ***10.5.2.*** » et « ***10.5.4.*** » de la classe A « ***10.*** » et 2 sous domaines du domaine : ***com.net***. Sur la machine qui fait office de DNS primaire, on trouve les deux tables suivantes : (qui répertorient l'ensemble des machines de l'entreprise.)

s1.com.net

```
@       IN SOA    dns (
                  admin.com.net.
                   27
                   3600
                   360
                   360000
                   36000 )
        IN NS     dns
        IN NS     dns.s2.com.net.
        IN MX     1 mail.s2.com.net.
dns     IN A      10.5.2.2
dns2    IN CNAME  dns.s2.com.net.
www     IN A      10.5.2.1
gate    IN A      10.5.2.3
        IN A      10.5.4.8
```

s2.com.net

```
@       IN SOA    dns.s1.com.net. (
                  admin.com.net.
                   12
                   3600
                   360
                   360000
                   36000 )
        IN NS     dns.s1.com.net.
        IN NS     dns
        IN MX     1 mail
dns     IN A      10.5.4.7
www     IN A      10.5.4.5
mail    IN A      10.5.4.6
gate    IN CNAME  gate.s1.com.net.
ftp     IN CNAME  www
```

Q14 :Donnez la liste des machines de l'entreprise avec pour chaque machine sa ou ses adresses IP, sa ou ses noms complets (c'est à dire avec le domaine). Vous soulignerez le nom canonique.

2,0

Nom canonique	*Alias*	*Adresse*	*Remarque :*
www.s1.com.net		*10.5.2.1*	
dns.s1.com.net		*10.5.2.2*	*Serveur DNS primaire*
gate.s1.com.net	*gate.s2.com.net*	*10.5.2.3* *10.5.4.8*	
dns.s2.com.net	*dns2.s1.com.net*	*10.5.4.7*	*Serveur DNS secondaire*
www.s2.com.net	*ftp.s2.com.net*	*10.5.4.5*	
mail.s2.com.net		*10.5.4.6*	*Serveur SMTP*

Q16 :Donnez le contenu de la table inverse « 2.5.10.in-addr.arpa ».

2,0

On reprend les valeurs de SOA et NS des autres tables DNS de l'entreprise :

```
@       IN SOA    dns.s1.com.net. (
                  admin.com.net.
                   1
                   3600
                   360
                   360000
                   36000 )
        IN NS     dns.s1.com.net.
        IN NS     dns.s2.com.net.
1       IN PTR    www.s1.com.net.
2       IN PTR    dns.s1.com.net.
3       IN PTR    gate.s1.com.net.
```

Comme on est dans la table « 2.5.10.in-addr.arpa » et non dans la table « s1.com.net » ou « s2.com.net », il faut spécifier les noms canoniques en entier (sous forme FQND : « Full Qualified Name Domain »).